

REMARKS

The Examiner rejected claims 1-4, 9, 14-25 and 27-29 under 35 U.S.C. §102(e) as allegedly being anticipated by US Patent Publication No. 2002/0112185 A1 to Hodges.

The Examiner rejected claims 13 and 16 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hodges (US Publication No. 2002/0112185 A1) in view of US Patent No. 6,167,520 to Touboul.

Applicants respectfully traverse the §102(e) and §103(a) rejections with the following arguments.

35 U.S.C. §102(e)

The Examiner rejected claims 1-4, 9, 14-25 and 27-29 under 35 U.S.C. §102(e) as allegedly being anticipated by US Patent Publication No. 2002/0112185 A1 to Hodges.

Claims 1-4, 20-25, and 27-29

Applicants respectfully contend that Hodges does not anticipate claim 1, because Hodges does not teach each and every feature of claim 1.

A first reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: "awaiting an occurrence of a next update time of the intrusion detection system, said next update time being a time at which at least one validity condition of the at least one business rule is checked" (emphasis added).

The Examiner argues (in "Response to Arguments"): "Hodges does teach of waiting for an next update time at which one validity condition is checked see Par 0012 & Par 0014 & Par 0132".

In response, Applicants respectfully contend Hodges, Pars. 0012 and 0014 merely discloses detection of an access system event, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". Furthermore, Hodges, Par. 0132 merely discloses "timing conditions restricting the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked, as required by claim 1. In addition, Hodges, Par. 0132

discusses timing conditions in conjunction with application of an authorization rule, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". In other words, Hodges does not teach use of an update time and awaiting an occurrence of the update time. Applicants respectively request that the Examiner explain with clarity where Hodges allegedly teaches use of an update time.

A second reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: **"responsive to the occurrence of the next update time, checking the at least one validity condition of the at least one business rule to determine whether a provision of any business rule of the at least one business rule is a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked, said newly operative provision prescribing an alteration of an intrusion set that the provision applies to"** (emphasis added).

The Examiner argues (in "Response to Arguments"): "And further is responsive to the occurrence of a business rule see Par 0015 & Abstract; also Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221. Hodges talks of monitoring for an event(waiting for an event) and in addition he says that it could be any suitable event(includes time) see Par 0013-0015."

In response, Applicants maintain that none of the Examiner's citations indicate checking the at least one validity condition of the at least one business rule **responsive to the occurrence**

of the next update time. Applicants respectively request that the Examiner explain with clarity where Hodges allegedly teaches said "responsive to the occurrence of the next update time".

In further response, Applicants that the Examiner has incorrectly interpreted Hodges, Pars. 0220-0221. The Examiner alleges: "Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221", which is incorrect. Applicants assert that Hodges, Par. 0220 merely checks the authorization rule cache 572 for the existence therein of authorization rules associated with a requested resource. Hodges, Pars. 0220-0221 does not perform checking to see if the rule is "new" (i.e., "a newly operative provision that has first become operative or gone into effect since an occurrence of a last previous update time at which the at least one validity condition of the at least one business rule was checked"). Applicants respectively request that the Examiner explain with clarity where Hodges allegedly teaches said checking to see if the at least one validity condition is a newly operative provision under the constraints recited in claim 1.

A third reason why Hodges does not anticipate claim 1 is that Hodges does not teach the feature: "if the checked provision is the newly operative provision that applies to the intrusion set, then altering the intrusion set according to the newly operative provision".

The Examiner argues that Hodges teaches the preceding feature of claim 1 in Pars. 0200-0201. In response, Applicants contend that Hodges, Pars. 0220-0221 merely teaches: "In step 1494, authorization module 542 determines whether one or more authorization rules associated with the requested resource are found in authorization rule cache 572. If one or more rules are

found, authorization module 542 proceeds to step 1496." Applicants note that step 1496 of FIG. 38 "reads the first authorization rule associated with the requested resource from authorization rule cache 572", which is not an altering of an intrusion set as alleged by the Examiner.

The Examiner also argues that Hodges teaches the preceding feature of claim 1 in the Abstract. In response, Applicants contend that Hodges' Abstract recites: "The system detects an access system event in the access system and determines whether the access system event is of a type that is being monitored. If the access system event is of a type that is being monitored, the system reports information about the access system event. This information can be used by a rules engine or other process to determine if the access system event was part of an attempted intrusion of the access system.", which is not a teaching of an altering of an intrusion set as alleged by the Examiner.

Based on the preceding arguments, Applicants respectfully maintain that Hodges does not anticipate claim 1, and that claim 1 is in condition for allowance. Since claims 2-4, 20-25 and 27-29 depend from claim 1, Applicants contend that claims 2-4, 20-25 and 27-29 are likewise in condition for allowance.

In addition with respect to claim 3, Hodges does not teach "wherein the validity condition is a network validity condition". Applicants maintain that the Examiner's citation of Hodges, Par. 0008 merely discusses prior art and does not state anything about Hodges' invention that the Examiner relies on. Moreover, the content in Hodges, Par. 0008 does not teach a network validity condition of a business rule used in conjunction with an intrusion detection system, as

required by claim 3.

In addition with respect to claims 23-25, Hodges does not teach "wherein the next update time is a scheduled time" (claim 23); "wherein the next update time is one update time of a plurality of update times that occur substantially periodically" (claim 24); and, wherein the next update time is a computed update time" (claim 25). The Examiner's citation of Hodges, Par. 0132 is not persuasive, because Hodges, Par. 0132 discloses "timing conditions restricting the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked as required in claims 23-25.

In addition with respect to claims 27-29, Hodges does not teach that the step of altering the intrusion set includes the step of altering: a threshold of the intrusion set (claim 27); an action of the intrusion set (claim 28); and a weight of the intrusion set (claim 29). The Examiner's citation of Hodges, Pars. 0107 and 0131 do not teach the preceding features of claims 27-29. Applicants respectfully request that the Examiner explain with clarity where Hodges, Pars. 0107 and 0131 allegedly teaches the preceding features of claims 27-29.

Claims 9 and 14-19

Applicants respectfully contend that Hodges does not anticipate claim 9, because Hodges does not teach each and every feature of claim 9.

A first reason why Hodges does not anticipate claim 9 is that Hodges does not teach the feature: "awaiting an update time of the intrusion detection system," (emphasis added).

The Examiner argues (in "Response to Arguments"): "Hodges does teach of waiting for an next update time at which one validity condition is checked see Par 0012 & Par 0014 & Par 0132".

In response, Applicants respectfully contend Hodges, Pars. 0012 and 0014 merely discloses detection of an access system event, and most certainly does not disclose "awaiting an occurrence of an update time of the intrusion detection system". Furthermore, Hodges, Par. 0132 merely discloses "timing conditions restricting] the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked, as required by claim 9. In addition, Hodges, Par. 0132 discusses timing conditions in conjunction with application of an authorization rule, and most certainly does not disclose "awaiting an occurrence of a next update time of the intrusion detection system". In other words, Hodges does not teach use of an update time and awaiting an occurrence of the update time. Applicants respectfully request that the Examiner explain with clarity where Hodges allegedly teaches use of an update time.

A second reason why Hodges does not anticipate claim 9 is that Hodges does not teach the feature: "responsive to the occurrence of an update time, checking validity conditions of the set of business rules to determine whether a provision of any of the set of business rules is a newly operative provision" (emphasis added).

The Examiner argues (in "Response to Arguments"): "And further is responsive to the

occurrence of a business rule see Par 0015 & Abstract; also Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221. Hodges talks of monitoring for an event(waiting for an event) and in addition he says that it could be any suitable event(includes time) see Par 0013-0015."

In response, Applicants maintain that none of the Examiner's citations indicate checking validity conditions of the set of business rules responsive to the occurrence of the an update time. Applicants respectively request that the Examiner explain with clarity where Hodges allegedly teaches said "responsive to the occurrence of an update time".

In further response, Applicants that the Examiner has incorrectly interpreted Hodges, Pars. 0220-0221. The Examiner alleges: "Hodges discloses of adding to the intrusion set and checking to see if it is new by comparing the rule with the cache and further retrieving from Directory see Par 0220 & Par 0221", which is incorrect. Applicants assert that Hodges, Par. 0220 merely checks the authorization rule cache 572 for the existence therein of authorization rules associated with a requested resource. Hodges, Pars. 0220-0221 does not perform checking to see if the rule is "new" (i.e., "a newly operative provision"). Applicants respectively request that the Examiner explain with clarity where Hodges allegedly teaches said checking to see if the at least one validity condition is a newly operative provision as recited in claim 9.

A third reason why Hodges does not anticipate claim 9 is that Hodges does not teach the feature: "if the new provision applies to the intrusion set, altering the intrusion set according to the newly operative provision".

The Examiner argues that Hodges teaches the preceding feature of claim 1 in Pars. 0200-0201. In response, Applicants contend that Hodges, Pars. 0220-0221 merely teaches: "In step 1494, authorization module 542 determines whether one or more authorization rules associated with the requested resource are found in authorization rule cache 572. If one or more rules are found, authorization module 542 proceeds to step 1496." Applicants note that step 1496 of FIG. 38 "reads the first authorization rule associated with the requested resource from authorization rule cache 572", which is not an altering of an intrusion set as alleged by the Examiner.

The Examiner also argues that Hodges teaches the preceding feature of claim 1 in the Abstract. In response, Applicants contend that Hodges' Abstract recites: "The system detects an access system event in the access system and determines whether the access system event is of a type that is being monitored. If the access system event is of a type that is being monitored, the system reports information about the access system event. This information can be used by a rules engine or other process to determine if the access system event was part of an attempted intrusion of the access system", which is not a teaching of an altering of an intrusion set as alleged by the Examiner.

Based on the preceding arguments, Applicants respectfully maintain that Hodges does not anticipate claim 9, and that claim 9 is in condition for allowance. Since claims 14-19 depend from claim 9, Applicants contend that claims 14-19 are likewise in condition for allowance.

In addition with respect to claims 14-16, Hodges does not teach that the step of altering the intrusion set includes the step of altering: a threshold of the intrusion set (claim 14); an action

of the intrusion set (claim 15); and a weight of the intrusion set (claim 16). The Examiner's citation of Hodges, Pars. 0107 and 0131 do not teach the preceding features of claims 14-16. Applicants respectively request that the Examiner explain with clarity where Hodges, Pars. 0107 and 0131 allegedly teaches the preceding features of claims 14-16.

In addition with respect to claims 17-19, Hodges does not teach "wherein the update time is a scheduled time" (claim 17); "wherein the update time is one update time of a plurality of update times that occur substantially periodically" (claim 18); and, wherein the update time is a computed update time" (claim 19). The Examiner's citation of Hodges, Par. 0132 is not persuasive, because Hodges, Par. 0132 discloses "timing conditions restricting] the time when the authorization rule is in effect", and Hodges, Par. 0132 does not disclose update times when the validity conditions of the at least one business rule is checked as required in claims 17-19.

35 U.S.C. §103(a)

The Examiner rejected claims 13 and 26 under 35 U.S.C. §103(a) as allegedly being unpatentable over Hodges (US Publication No. 2002/0112185 A1) in view of US Patent No. 6,167,520 to Touboul.

Since claim 13 depends from claim 9 which Applicants have argued *supra* to not be anticipated by Hodges, Applicants contend that claim 13 is not unpatentable over Hodges in view of Touboul under 35 U.S.C. §103(a).

Since claim 26 depends from claim 1 which Applicants have argued *supra* to not be anticipated by Hodges, Applicants contend that claim 26 is not unpatentable over Hodges in view of Touboul under 35 U.S.C. §103(a)

In addition with respect to claims 13 and 26, Applicants respectfully contend that Hodges does not teach or suggest the feature: "wherein the step of altering the intrusion set includes the step of altering a signature of the intrusion set".

The Examiner argues: "Hodges does not disclose the step of altering a signature of the intrusion set. However, Touboul does suggest the altering of signature as Downloadables are stamped with an signature and further different downloads having different signature see Col 1 Line 52-64. It would be obvious to one having ordinary skill in the art at the time of the invention to include a step of altering an signature of the intrusion set in order for protecting data from hostile agents see Column 1 Line 62-63."

In response, Applicants respectfully contend that the Examiner's argument is not persuasive, because Touboul, col. 1, lines 52-64 does not suggest altering a digital signature of

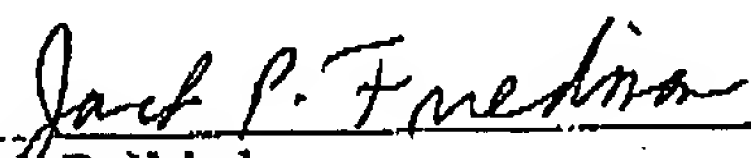
Downloadables. In fact, Touboul, col. 1, lines 62-63 states that "a digital signature does not guarantee that a Downloadable is harmless". While Touboul col. 1, lines 63-64 states that "a system and method are needed for protecting clients from hostile Downloadables", Touboul does not teach or suggest that altering a digital signature will protect clients from hostile Downloadables."

Accordingly, Applicants maintain that the Examiner has not established a *prima facie* case of obviousness in relation to claims 13 and 26.

CONCLUSION

Based on the preceding arguments, Applicants respectfully believe that all pending claims and the entire application meet the acceptance criteria for allowance and therefore request favorable action. If the Examiner believes that anything further would be helpful to place the application in better condition for allowance, Applicants invites the Examiner to contact Applicants' representative at the telephone number listed below. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Date: 06/29/2005



Jack P. Friedman
Registration No. 44,688

Schmeiser, Olsen & Watts
3 Lear Jet Lane, Suite 201
Latham, New York 12110
(518) 220-1850